# National Privacy Research Strategy Workshop, Feb 2015

# Summary

## Workshop Summary

The Federal Networking and Information Technology Research and Development (NITRD) Program held a workshop as part of the development of the National Privacy Research Strategy, during February 18-20, 2015 in Arlington, Virginia. Organized by the National Coordination Office for NITRD, the workshop's purpose was to explore privacy needs across the private and public sectors, objectives that could guide federal privacy research, and innovative research directions to preserving and managing privacy in cyberspace.

## Background

The United States is in the midst of a global economic and societal transformation. This transformation is being driven by a burgeoning networking and information technology (NIT) ecosystem that is being designed to capture and store vast amounts of data as well as transfer, combine, and mine the data to generate new knowledge that can improve the lives of customers, citizens, and families. The transformation is visible in, for example, the growing availability of social media, online education, and mobile health services. With increasing broadband penetration and performance, more powerful edge devices such as smart phones, and with advances in the "Internet of Things", this transformation will only accelerate. Indeed, new services are already emerging in emergency response, environmental monitoring, and in "smart city" ideas such as energy control, automobile traffic shaping, and aging in place. It is hard to overestimate the opportunities for innovation that lie ahead of us.

Maximizing the value of such systems depends upon them being integrated into our everyday lives, but doing so presents privacy risks that threaten this transformation and its promised benefits. Thus, understanding the nature of privacy and how it can be engaged is of central importance.

Privacy is a complex societal issue where it is necessary for us to work together despite our individual and cultural differences. While privacy is, in some ways, related to security - people often conflate the two ideas - privacy is less well understood and so harder to address. For example, while one can rightly focus research in cybersecurity on how to find ways to get ahead of the criminal elements that attack our cyberinfrastructure, there is often no such clear distinction between good and bad in regards to privacy - it's all of us in this together, struggling to understand the consequences of specific actions. Indeed, because of the rapid adoption of social media and the role it has taken in people's lives, one often hears the fatalistic view that "privacy is dead". This sentiment is understandable but misguided:

now is the time that we must work together to understand the emerging risks to our privacy, and how they can be mitigated.

The White House[1] and The President's Council of Advisors on Science and Technology[2] (PCAST) reports on big data and privacy, as well as PCAST 2013[3] and 2010[4] reports on NITRD[5] call for serious increases in investments for R&D in privacy-enhancing technologies and in encouraging multi-disciplinary research involving computer science, social science, and legal disciplines. Subsequently, the White House Office of Science and Technology Policy charged NITRD with the task of preparing a draft National Privacy Research Strategy (NPRS) that would provide a framework for coordinated research in privacy-enhancing technologies, in partnership with the private sector and interested citizens.

The National Privacy Research Strategy will present a set of research goals that the federal government distinguishes as being important in identifying and mitigating the risks to our privacy that arise from our NIT ecosystem. These goals will be chosen both to meet individual agency goals (e.g., the National Institute of Health's interests in the analysis of healthcare data, and the National Institute of Standards and Technology's goals in helping to codify engineering practices that control risks to privacy at the design stage) and to uncover the underlying social, behavioral, economic, and computer science principles of privacy. The goals will consider the entire privacy landscape, from how people understand it in different situations and how their resulting needs can be formally specified, to how these needs can be enforced, and to how mitigation and remediation can be accomplished should the required privacy be violated. The goals will look beyond the ideas of "locking down" information and refining Fair Information Practice Principles (FIPPs) to methods of controlling information in terms of the context it is used, and into ways that people can understand and control the privacy of their information in the face of changing technologies and contexts.

Organized by the National Coordination Office for NITRD, the workshop brought together government, academia, and industry experts to explore privacy needs across the private and public sectors, objectives that could guide privacy research, and innovative research directions to preserving and managing privacy in cyberspace. The workshop was structured as a series of panels to support open discussions among the panelists and attendees. The workshop discussions serve as input to the development of the National Privacy Research Strategy.

[1] "Big Data: Seizing Opportunities, Preserving Values," May 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

[2] "Big Data and Privacy: A Technological Perspective," May 2014, http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

[3] "Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology," January 2013, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd2013.pdf

[4] "Designing a Digital Future: Federally Funded Research and Development Networking and Information Technology," December 2010, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf

[5] NITRD Program provides a framework in which many US Government agencies to coordinate networking and information technology research and development efforts. More information is available at http://www.nitrd.gov

## Workshop Structure and Agenda

The first day of the workshop focused on discussing and understanding privacy and privacy challenges from four different perspectives:

- Government perspective: the government is responsible for creating and executing privacy laws/regulations and supporting privacy requirements of such laws. The government is also responsible for conducting law enforcement and providing national defense while protecting privacy.
- Individual perspective: this perspective is characterized by concerns by individuals about the collection and use of personal data.
- Commerce perspective: the pursuit of business opportunities that involve collection and use of personal information, in marketing, big data analytics, etc.
- Societal perspective: this perspective considers effects from the loss of privacy on society as a whole, such as erosion of freedom, self-censoring, or informational discrimination. Other concerns include how to balance IT innovation with privacy protection.

The second day of the workshop focused on examining prospective privacy research areas and objectives. The structure of the second day corresponded to the social/sociological approach to understanding privacy:

- Social and institutional structures create context for privacy norms, expectations, and rules. The context helps define circles or groups, each with their own privacy norms.
- There are many such groups, such as social (family, friends, etc.), professional (employment, medical, etc.), commerce (on-line retail transactions), government, etc. Groups have different norms/expectations/rules for what is acceptable, and group norms may be dynamic.
- Violations of privacy occur when deviations from the norms of a particular group take place.
- Different groups can have varying controls of information flows/disclosures.

Following the social/sociological framework of privacy, three areas of research inquiry were organized for the workshop:

- <u>Privacy Expectations</u>: methods and technologies that will provide the capabilities to define, capture, and operationalize the norms, expectations, and rules for acceptable activities, information disclosure, and data flows in the digital realm.
- <u>Privacy Violations</u>: methods and technologies for understanding, detecting, assessing, and reasoning about deviations from norms/expectations/rules, and harms.
- <u>Privacy Controls</u>: methods and technologies to manage and mitigate risk in order to satisfy pertinent privacy norms/expectations/rules and prevent privacy violations.

## Workshop Agenda

| **National Privacy Research Strategy Workshop**<br>**February 18-20, 2015**<br>**SRI International, 1100 Wilson Blvd, Arlington, VA 22209** | |
|---|---|
| 9:00 – 9:30 | Introduction, workshop motivation and objectives, Tomas Vagoun, NCO/NITRD |
| 9:30 – 10:15 | Keynote<br>David Medine, Chairman, Privacy and Civil Liberties Oversight Board (PCLOB) |
| 10:15 – 10:45 | Break |
| 10:45 – 12:00 | Panel: Privacy Perspective: Government<br>• Claire Barrett, Chief Privacy Officer, DOT<br>• Alexander Joel, Civil Liberties Protection Officer, ODNI<br>• Lucia Savage, Chief Privacy Officer, HHS/ONC<br>• Ashkan Soltani, Chief Technologist, FTC<br>• Moderator: Daniel Weitzner, MIT |
| 12:00 – 1:00 | Lunch break |
| 1:00 – 2:15 | Panel: Privacy Perspective: Individual/Consumer<br>• Mary Culnan, Bentley University; Future of Privacy Forum<br>• Alfred Kobsa, University of California, Irvine<br>• Stuart Pratt, Consumer Data Industry Association<br>• Joseph Turow, University of Pennsylvania<br>• Moderator: Jessica Lyon, FTC |
| 2:15 – 3:30 | Panel: Privacy Perspective: Commerce<br>• Jules Cohen, Microsoft<br>• Mark MacCarthy, Software Information Industry Association<br>• Mona Vernon, Thomson Reuters<br>• Claire Vishik, Intel Corporation<br>• Moderator: Stuart Shapiro, MITRE |
| 3:30 – 3:45 | Break |
| 3:45 – 5:00 | Panel: Privacy Perspective: Society<br>• Alvaro Bedoya, Georgetown Law<br>• Dawn Diedrich, Georgia Bureau of Investigation<br>• Susan Landau, Worcester Polytechnic Institute<br>• Daniel Weitzner, MIT<br>• Moderator: Gregg Motta, FBI |

| **February 19, 2015** | |
|---|---|
| 8:45 – 9:00 am | Introduction to second day |
| 9:00 – 9:30 | Spotlight Presentation: Report from the 2014 NSF Workshop on Big Data Security and Privacy, Bhavani Thuraisingham, UT Dallas |
| 9:30 – 11:00 | Panel: Privacy Expectations Research Area<br>• Lorrie Cranor, CMU<br>• Carl Gunter, University of Illinois<br>• Helen Nissenbaum, NYU<br>• Stuart Shapiro, MITRE<br>• Moderator: Chris Clifton, NSF |
| 11:00 – 11:15 | Break |
| 11:15 – 11:45 | Spotlight Presentation: Project Brandeis, John Launchbury, DARPA |
| 11:45 – 1:00 | Lunch break |
| 1:00 – 1:30 | Spotlight Presentation: Advances in Secure Multiparty Computation and Suggestions for Further Research, Konrad Vesey, Elkridge Security |
| 1:30 – 3:00 | Panel: Privacy Violations Research Area<br>• Dixie Baker, Martin, Blanck & Associates; HHS Health IT Standards Advisory Committee<br>• Pam Dixon, World Privacy Forum<br>• Deirdre Mulligan, Berkeley<br>• Sam Weber, Software Engineering Institute<br>• Moderator: Christa Jones, US Census Bureau |
| 3:00 – 3:15 | Break |
| 3:15 – 3:45 | Spotlight Presentation: Privacy Engineering, Naomi Lefkovitz, NIST |
| 3:45 – 5:15 | Panel: Privacy Controls Research Area<br>• Dawn Jutla, Saint Mary’s University; Chair, OASIS Privacy by Design Documentation for Software Engineers TC<br>• Tal Rabin, IBM T.J. Watson Research Center<br>• Aaron Roth, University of Pennsylvania<br>• Bhavani Thuraisingham, UT Dallas<br>• Moderator: Naomi Lefkovitz, NIST |

| **February 20, 2015** | |
|---|---|
| 8:45 – 9:00 am | Introduction to third day |
| 9:00 – 9:30 | Spotlight Presentation: Developing the Science of Privacy, Rebecca Richards, NSA |
| 9:30 – 11:00 | Panel: Privacy Research Objectives<br>• Alvaro Bedoya, Georgetown Law<br>• Jules Cohen, Microsoft<br>• Latanya Sweeney, Harvard<br>• Daniel Weitzner, MIT<br>• Moderator: Marjory Blumenthal, OSTP |
| 11:00 – 11:15 | Break |
| 11:15 – 12:00 | Workshop Summary |
| 12:00 pm | Adjourn |

## Workshop Discussions

The following summaries highlight concerns, ideas, and points of discussion during the workshop panels. The summaries are views of the workshop panelists and participants and do not imply any particular position by the government agencies. The summaries are intended to capture discussion points relevant to the development of a prospective National Privacy Research Strategy.

### Keynote

David Medine, Chairman of the Privacy and Civil Liberties Oversight Board (PCLOB) gave the opening keynote.

Summary:

- Privacy is a multidisciplinary concern
- Fair Information Practice Principles (FIPPs) need to be revised
    - Reexamine how individuals can meaningfully participate in cyberspace, when so much data is or can be collected about individuals.
    - Notice and consent is not working; consumers are not exercising informed consent; what is a good consent model for individuals?
- Focused collection
    - How to collect just the right amount of information for the intended purpose?
- Efficacy of government's collections
    - We need methodology for understanding the efficacy of government data collection programs.
- Encryption
    - How does encryption affect the balance between public's privacy and law enforcement?
    - Are there better ways to preserve privacy without thwarting law enforcement (LE) and national security (NS)?
- Collection-restrictions vs. use-restrictions of data
    - Are there effective use-restrictions?
- Predictive algorithms
    - Discrimination remains a concern with predictive algorithms.
    - Are predictive algorithms appropriate in the government space? Potential harms from false positives in LE and NS context could be more severe than in the consumer space.
    - How can we evaluate (as a black box) predictive algorithms?

### Panel: Privacy Perspective: Government

Panel framing: The privacy perspective by the Government is characterized by Government's responsibilities in preventing anticompetitive and deceptive business practices, law enforcement, and national defense while protecting privacy and civil liberties. Formulating and enacting privacy laws, while a critical function of the government, was not a focus of this panel.

Summary:

- FIPPs
    - FIPPs can stay as-is; however, we need to differentiate between FIPP principles (which provide valuable guidance) and how to implement/effectuate the principles—which can evolve and change.
- Algorithms
    - Algorithmic transparency research is needed; for anti-discrimination assessment and compliance with relevant rules and protections.
- Policy and technology
    - How can we connect rules and policies with quickly-changing technology and capabilities; what are the key principles and how to apply them as the technology evolves?
    - Are there basic principles that would apply to all federal agencies regarding privacy, and how would we map those principles to all agencies?
    - There is a subject-matter divide and a communication gap between policy/legal and technical camps; how can we make academic research outcomes accessible and understandable to the government decision makers?
    - We need sociological research about what do people expect from the government, and as compared to industry, regarding privacy.
- Government transparency
    - How can  transparency be enabled for the Intelligence Community?

## Panel: Privacy Perspective: Individual/Consumer

Panel framing: The individual/consumer privacy perspective is signified by the concerns by individuals regarding how information about them in cyberspace is collected and used.

Summary:

- Privacy notices
    - Privacy notices are too long, to legalistic, and are written as contracts to protect the company; there is no meaningful choice for customers anymore. Also, notices do not address secondary use of data.
    - We need more research on privacy notices: what format should they be in; what type of notices should be used in a given technology context (desktop, mobile, IoT, etc.).
    - We need to provide more education about privacy to people. There is a lack of understanding in the general population about the impact of IT on privacy.
    - Privacy self-management does not work; it is not realistic to expect individuals to be able to manage their privacy preferences across the spectrum of IT systems and services.
- Data collection practices

  - People have little understanding about data-use practices; the notion that people can make cost/benefit assessments regarding privacy and utility of data collections does not hold.
  - More research is needed on what is actually taking place in the industry regarding data collection practices.
  - More research is needed on what is the right transparency for data collections.
- Incentives
  - More research is needed to understand the effects and efficacy of incentives for good privacy.
  - Consumer privacy and societal benefits from data collection should be balanced. We should not limit technology innovation.

## Panel: Privacy Perspective: Commerce

Panel framing: The privacy perspective by commercial entities centers on the pursuit of business opportunities that involve the collection and use of personal information, in marketing, consumer services, healthcare, big data analytics, etc.

Summary:

- Trust
  - People will not use technologies they don't trust. Transparency and communication can help alleviate mistrust. Further research is needed to find effective ways to improve transparency for IT systems.
  - More research is needed in threat models and risk models related to privacy.
- Technology drivers
  - Increasingly, we live in a world surrounded by data generated by simple sensor and instruments (e.g. Internet of Things). On its own, the data may not pose privacy risks. However, in aggregate, privacy risks arise. How can privacy protections be incorporated into simple instruments and around machine-generated data?
  - As systems become interconnected with other systems, we need more research in privacy composition. Similarly, end-user products are often comprised from sub-elements that were created with different (or none) privacy considerations and full implications do not become clear until the product is in use.
  - More research is needed to evaluate the range of risks and exposures to privacy harms in the commercial space.
  - As technology proliferates, new and innovative technical means are needed to allow users to express/give consent and permissions.

## Panel: Privacy Perspective: Society

Panel framing: The society privacy perspective is an area of concerns about effects from the loss of privacy on the society as a whole, such as erosion of freedom, self-censoring, marketing-driven compartmentalization of people in cyberspace, informational discrimination, etc. Topics about how to balance IT innovation with privacy protection are also included.

Summary:

- Social objectives for privacy
    - Avoid chilling effects (when we know we are watched, we behave differently). Further research into chilling effects is needed.
    - Avoid totalitarianism (too much control by a single entity).
- Collection-limitations vs. use-limitations
    - Data collection is so prevalent that it is not realistic to impose meaningful controls on data collecting. We need to do more to control data use, such as better ways of auditing. Notice and consent is a simple idea, but use-control is more complex, because it depends on the use case—and so is much more complex to specify and control. Further research on what works/doesn't work in use-limitations is needed.
    - At the same time, we need to recognize that use-limitations have regrettable history (e.g. using the Census data to intern Japanese-American citizens).
    - Allowing fairly unrestricted data collections has preserved competition and innovation in consumer controls. Additional research in consumer controls is desirable.
    - Collection-limitations and use-limitations remain important to society and we need further research into both.
- US citizenship determination
    - A key basis for the legality of government bulk data-collection programs is how many US citizens could be affected (their private data collected). We need the ability to determine if a person is a US citizen and the percentage of US citizens potentially affected by the bulk data-collection program.
- Societal
    - Trust in law enforcement is critical for a healthy society. There should be limitations on what the government can collect, as well as use-limitation on the collected data. There needs to also be transparency about the effectiveness of government collection programs.

## Panel: Privacy Expectations Research Area

Panel framing: Privacy begins with our understanding of the norms, expectations, and rules for what is acceptable in a particular context. Research within the Privacy Expectations Area seeks to develop methods and technologies that will provide the capabilities to define, capture, and operationalize the norms, expectations, and rules for acceptable activities, information disclosure, and data flows in the digital realm, while supporting the establishment of a particular context (privacy group).

Summary:

- A productive society needs information sharing. However, the notion that we need to give up some measure of privacy in exchange for some value should be contested. For example, a visit to a physician involves sharing of information but does not diminish privacy.
- Expectations are a function of the ongoing interactions with socio-technical systems. It may be difficult to study expectations as something that is independent from its surrounding. Perhaps “norms” would be a better term for this research area.
- Research goals
    - We need privacy technology research in: derive (logic) existing norms, to model (formally represent) them and how to implement them (crypto, architecture, permissions), in order to detect violations and enforce informational norms.
    - Designers need to understand technological systems as interpretative model/process and we need to find ways to push engagement (by stakeholders) upstream in the development process. We need to rethink/expand participation in the development process (e.g. an IRB Model for BD analytics, and other systems that touch on privacy)
    - Further research is needed on how people form expectations, and to help people understand when technology may create privacy surprises.

## Panel: Privacy Violations Research Area

Panel framing: Privacy violations arise when deviations from the norms of a particular privacy/context group occur. Research within the Privacy Violations Area seeks to develop methods and technologies for understanding, detecting, assessing, and reasoning about deviations from norms/expectations/rules, and harms that may occur as a consequence.

Summary:

- How do we determine that something is a privacy violation, given that a violation is dependent on the context, which varies between individuals and is dynamic?
- Developing methods and technologies for reasoning about privacy violations requires that we connect two bodies of work:
    - Privacy through law and philosophy: for example, right to be left alone, limiting access to the self, secrecy, zone of autonomous decision making, intimacy, personhood
    - Privacy support from computer science: such as, anonymity, confidentiality, requirements derived from privacy laws, access controls
    - Major gaps remain in how to connect these domains
- Privacy technologies need to accommodate variations of privacy among individuals and how those views changes. One area for further research is in the area of consent, specifically how more granular consent could be given, how the consent could remain associated with relevant data, and how consent could be revoked.

- Further research is needed in how easy or difficult it is to re-identify subjects from data sets that have been deemed de-identified.
- Algorithmic transparency is an area of growing importance that requires further study. How do we establish if an algorithm is fair?
- What are the effective penalties for harm done by privacy violations? Further research is needed to evaluate the impact of monetary fines vs. public disclosures (e.g. breach notifications).

## Panel: Privacy Controls Research Area

Panel framing: Within the Privacy Controls Area, research seeks to develop methods and technologies to manage and mitigate risk in order to satisfy pertinent privacy norms/expectations/rules and prevent privacy violations.

Summary:

- Differential privacy offers, in theory, a wide range of statistical analysis methods; however, there are practical limitations to what can be done with differential privacy techniques today. Further research is needed in this area.
- A number of privacy controls exist already. What is missing are architectures or frameworks that will enable designers to consider risk, utility, and cost in selecting proper controls.
- Software engineering needs to evolve to allow us to capture and embed privacy into software designs and projects.
- Incentives are a key challenge to a more effective deployment and use of privacy controls. Currently, companies have minimal motivation to improve privacy and much more to gain from collecting as much data as desired.

## Panel: Privacy Research Objectives

Panel framing: The federal privacy research strategy should describe the vision of future capabilities that will be made possible with the research, establish objectives and prioritization guidance for federally-funded privacy research, provide a framework for coordinating R&D in privacy-enhancing technologies, and encourage multi-disciplinary research that recognizes the responsibilities of the Government, the needs of society, and enhances opportunities for innovation in the digital realm. Because privacy is a social construct, the strategy should also be clear on what social needs and values will guide the research.

Summary:

- National strategy for privacy research needs to connect academic research with policy development. Most researchers are working on solutions that can only be put into practice with major upheaval in policies and laws. Even if new and better methods and tools are created, there is no reason to believe that they would be adopted, if there are no incentives or requirements for their adoption.

- Privacy research is an applied field; hence research funding should put priority on engagement with practical problems. Naturally, practical engagements require more people, time, resources than theoretical research.
- Privacy research needs to be also connected with law-making and Congress. Law-making process today is significantly disconnected from an understanding of technologies and their impact on privacy.
- One of the contributions of the Strategy should be in creating bridges between academic research, policy development, and law-making. The Strategy should address research objectives but also address deficiencies in institutional structures that are impeding progress (e.g. disincentives for multidisciplinary academic research, for applied research, for making practical impact).
- One of the privacy research objectives should be how to treat policy as a first class computational object, so that we can include a policy in the computing with the data if affects.
- Another major challenge for research is to understand the right level of interaction of humans with privacy automation.
- Research in privacy needs to be a multidisciplinary effort (computing, social science, economics, and law). Framing of the research should be based on practical issues.
- A future world of ubiquitous data collection is something we should avoid.

## Workshop Attendees

| | |
|---|---|
| Alvisi, Lorenzo | University of Texas at Austin |
| Baker, Dixie | Martin, Blanck & Associates and HHS Health IT Standards Advisory Committee |
| Bachman, Robin | US Census Bureau |
| Banks, Lerone | Federal Trade Commission |
| Barrett, Claire | US Department of Transportation |
| Bedoya, Alvaro | Georgetown Law |
| Benoy, Benjamin | National Security Agency |
| Blumenthal, Marjory | Office of Science and Technology Policy |
| Bogner, Kathleen | Office of the Director of National Intelligence |
| Brooks, Sean | National Institute of Standards and Technology |
| Bryant, Randy | Office of Science and Technology Policy |
| Clifton, Chris | National Science Foundation |
| Cohen, Jules | Microsoft |
| Cranor, Lorrie | Carnegie Mellon University |
| Culnan, Mary | Bentley University and Future of Privacy Forum |
| David Balenson | Department of Homeland Security/S&T |
| DePersia, Trent | Department of Homeland Security/S&T |
| Diedrich, Dawn | Georgia Bureau of Investigation |
| Dixon, Pam | World Privacy Forum |
| Doray, Ed | US Northern Command |
| Ellman, Eric | Consumer Data Industry Association |
| Epstein, Jeremy | National Science Foundation |
| Fiedelholtz, Glenn | Department of Homeland Security/OCIA |
| Garfinkel, Simson | National Institute of Standards and Technology |
| Gavilia, Patricia | Office of the Director of National Intelligence |
| Goolsby, Rebecca | Office of Naval Research |
| Gunter, Carl | University of Illinois |
| Hager, Gregory | Johns Hopkins University and Computing Community Consortium |
| Harmsen, Meg | National Coordination Office/NITRD |
| Hessman, Jeri | Defense Advanced Research Projects Agency |
| Higa-Smith, Karyn | Department of Homeland Security/S&T |
| Joel, Alexander | Office of the Director of National Intelligence |
| Jones, Christa | US Census Bureau |
| Jutla, Dawn | Saint Mary's University, Canada and OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC |
| Kelly, Anthony | National Science Foundation |

| | |
|---|---|
| Kobsa, Alfred | University of California, Irvine |
| Landau, Susan | Worcester Polytechnic Institute |
| Landwehr, Carl | Consultant to ODNI |
| Launchbury, John | Defense Advanced Research Projects Agency |
| Lefkovitz, Naomi | National Institute of Standards and Technology |
| Lyon, Jessica | Federal Trade Commission |
| MacCarthy, Mark | Software Information Industry Association |
| Marcos, David | National Security Agency |
| Marzullo, Keith | National Science Foundation |
| Medine, David | Privacy and Civil Liberties Oversight Board |
| Motta, Gregory | Federal Bureau of Investigation |
| Mulligan, Deirdre | University of California, Berkeley |
| Nguyen, Tristan | Air Force Office of Scientific Research |
| Nissenbaum, Helen | New York University |
| Pratt, Stuart | Consumer Data Industry Association |
| Rabin, Tal | IBM T.J. Watson Research Center |
| Rawlings-Goss, Renata | National Science Foundation |
| Richards, Rebecca | National Security Agency |
| Roth, Aaron | University of Pennsylvania |
| Salow, Heidi | Thomson Reuters |
| Savage, Lucia | Department of Health and Human Services/ONC |
| Shapiro, Stuart | MITRE Corporation |
| Soltani, Ashkan | Federal Trade Commission |
| Sullivan, Eugene | National Security Agency |
| Sweeney, Latanya | Harvard University |
| Thuraisingham, Bhavani | University of Texas at Dallas |
| Triplett, Ryan | Department of Homeland Security/S&T |
| Turow, Joseph | University of Pennsylvania |
| Vagoun, Tomas | National Coordination Office/NITRD |
| Vernon, Mona | Thomson Reuters |
| Vesey, Konrad | Elkridge Security |
| Vishik, Claire | Intel Corporation |
| Wachter, Ralph | National Science Foundation |
| Weber, Sam | Software Engineering Institute |
| Weitzner, Daniel | Massachusetts Institute of Technology |
| Xu, Heng | National Science Foundation |
| Zhao, Fen | National Science Foundation |